CTIIC is a small, multiagency center that works to increase the speed at which the US Government recognizes significant cyber activity is threatened or occurring so decisionmakers can act to prevent or minimize damage to US national interests. It is an integration point where analysts scrutinize fragments of cyber threat information produced by network defenders, Intelligence Community, law enforcement, incident responders, and non-Government sources; make connections; place the activity in context; call attention to significant activity; and work with partners to develop whole-of-government approaches to mitigate or counter the threat.

ODNI and the agencies that produce cyber threat intelligence designed CTIIC so that it supports, but does not duplicate, the work of other centers and agencies.

• CTIIC does not collect. It integrates and highlights information and expertise from around the community.
• It is not operational. CTIIC supports operators by ensuring they have the fullest possible threat picture and that parties with a range of tools and authorities are at the table when decisions are made.
• CTIIC has no direct liaison with the private sector. It works through agencies that do have those relationships and helps downgrade information and analysis they can share.
• The Center does not advocate a "CTIIC view." It produces community analysis on current threat issues by working with a wide set of experts (cyber, regional, technical, etc.) and by setting cyber activity in a broader context.